Astrotech Space Operations (ASO) Security Manual

Astrotech Space Operations

~~Only versions of this document on the web site are controlled~~Verify this is the current version before using.

ASTROTECH®

A SPACEHAB COMPANY

To the Employees of Astrotech Space Operations:

Astrotech Space Operations, Inc., has entered into a Security Agreement with the Department of Defense in order to have access to information that has been classified because of its importance to the National Defense. Many of our programs and activities are vital parts of the defense and security systems of the United States. Both Management and individual employees are responsible for properly safeguarding classified information. Our responsibility and obligation as an organization involved in such programs is to safeguard all information and material related to these programs.

This Security Manual identifies and describes the responsibilities and duties that result from being a part of the nation's defense team. Any employee having a question regarding their security responsibility should contact the Facility Security Officer. All of us have an obligation to see that our security practices are consistent with the best interests of the nation's defense program.

Sincerely,

– /s/John B. Satrom

John B. Satrom
Sr. Vice President & General Manager
Astrotech Space Operations, Inc.

TABLE OF CONTENTS

KEY DEFINITIONS

Access – The ability and opportunity to obtain knowledge of classified information.

Adverse Information – Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his/her ability to safeguard classified information may be impaired, or that his/her access to classified information clearly may not be in the interest of national security.

Authorized Person – A person who has a need-to-know for classified information in the performance of official duties and who has been granted personal clearance at the required level.

Automated Information System (AIS) – Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes computer software, firmware, and hardware.

Classified Contract – A classified contract is any contract that requires or will require access to classified information by the contractor or his/her employees in the performance of the contract. (A contract may be a classified contract even though the contract document is *not* classified.) The requirements prescribed for a "classified contract" also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Government Contracting Activity (GCA) program or project that requires access to classified information by a contractor.

Classification Guide – This is a document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified on a derivative basis. (The Contract Security Classification Specification provides Classification Guides to contractors.)

Classified Information – This term includes National Security Information, Restricted Data, and Formerly Restricted Data.

Closed Area – An area that meets the requirements of the National Industrial Security Program Operating Manual (NISPOM), as approved by the Cognizant Security Agency (CSA), for the purpose of safeguarding classified material that because of its size or nature, or operational necessity, *cannot* be adequately protected by the normal safeguards or stored during non-working hours in approved containers.

Cognizant Security Agency (CSA) – Agencies of the Executive Branch that have been authorized by E.O., 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. These agencies are: The Department of Defense (DoD), the Department of Energy (DoE), the Central Intelligence Agency (CIA), and the Nuclear Regulatory Commission.

Cognizant Security Office – Office or offices delegated by the Head of a CSA to administer industrial security in a contractor's facility on behalf of the CSA.

Compromise – The disclosure of classified information to an unauthorized person.

CONFIDENTIAL (C)– The designation that shall be applied to information or ~~material which~~material, which the unauthorized disclosure of could be reasonably expected to cause damage to national security.

Contracting Officer (CO) – Any government official who, in accordance with departmental or agency procedures, is currently designated as a Contracting Officer (CO) with the authority to enter into and administer contracts, and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the CO acting within the limits of his/her authority. For purposes of this procedure, the term *Contracting Officer* refers to the CO at the purchasing office who is identified as the Procuring Contracting Officer (PCO) and the CO at a contract administration office who is identified as the Administrative Contracting Officer (ACO). Normally, the responsibilities which this procedure assigns to the CO during the pre-contract, contract award, and post-contract stages of a classified procurement will be performed by the PCO, with the ACO performing those responsibilities which arise during the performance stages of a classified contract.

Custodian – Any individual who has possession of, or is otherwise charged with, the responsibility for the safeguarding or accounting of classified information.

Facility Security Clearance (FCL) – This is an administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

Foreign Interest – Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered, or incorporated under the laws of any country other than the United States (U.S.) or its possessions and trust territories, and any person who is *not* a citizen or national of the U.S.

Foreign National – Any person who is *not* a citizen or national of the United States.

Foreign Person – Any foreign interest and any U.S. person effectively owned or controlled by a foreign interest.

Letter of Consent (LOC) – This form is used by the CSA to notify a contractor that a Personal Security Clearance (PCL) or a Limited Access Authorization (LAA) has been granted to an employee.

Limited Access Authorization (LAA) – Security access authorization to CONFIDENTIAL or SECRET information granted to non-US Citizens requiring such limited access in the course of their regular duties.

Need-To-Know – This is a determination made by the possessor of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a classified contract or program.

Personnel Security Clearance (PCL) – Administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the PCL being granted.

Representatives of a Foreign Interest (RFI) – Citizen or national of the United States, who is acting as representative of a foreign interest. See Chapter 2, Section 3 of the NISPOM for further clarification.

SECRET (S) – The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Security Cognizance – The Government office assigned the responsibility for acting for CSAs in the discharge of industrial security responsibilities described in the NISPOM.

Security in Depth –Determination made by the CSA that a contractor's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility.

Security Violation – Failure to comply with the policies and procedures established by the NISPOM that reasonably could result in loss or compromise of classified information.

System Software – Computer programs that control, monitor, or facilitate use of the AIS; for example, operating systems, programming languages, communication, input-output control, sorts, security packages and other utility-type programs. Considered to also include off-the-shelf application packages obtained from manufacturers and commercial vendors, such as for word processing, spreadsheets, data base management, graphics, and computer-aided design.

Technical Data – Information governed by the International Traffic in Arms Regulation (ITAR) and the Export Administration Regulation (EAR). The ITAR controls the export of technical data that is inherently military in character. The EAR controls the export of technical data that has both military and civilian uses.

United States and its Territorial Areas – The 50 states, District of Columbia, Commonwealth of Puerto Rico, Guam, American Samoa, Virgin Islands, Trust Territory of the Pacific Island (also called Micronesia), Midway Island, Wake Island, Johnson Atoll, Kingman Reef, Swain's Island, and Palmyra Island.

Unauthorized Person – Any person *not* authorized to have access to specific classified information in accordance with the NISPOM.

United States – The 50 states and the District of Columbia.

United States Citizen (Native Born) – A person born in one of the following locations is considered to be a U.S. citizen for industrial security purposes: the 50 United States; District of Columbia; Puerto Rico; Guam; American Samoa; Northern Mariana Islands; U.S. Virgin Islands; Panama Canal Zone [if the father or mother (or both) was, or is, a citizen of the US]; Federated States of Micronesia; and Republic of the Marshall Islands.

ACRONYMS AND ABBREVIATIONS

(C)	CONFIDENTIAL
(S)	SECRET
(TS)	TOP SECRET
ACO	Administrative Contracting Officer
ADP	Automatic Data Processing
AIS	Automated Information System
ASO	Astrotech Space Operations
CAGE	Commercial and Government Entity Number (formally FSC)
CIA	Central Intelligence Agency
CNWDI	Critical Nuclear Weapon Design Information
CO	Contracting Officer
COMSEC	Communications Security
CSA	Cognizant Security Agency
CSO	Cognizant Security Office
DIS	Defense Investigative Service
DISCO	Defense Industrial Security Clearance Office
DoD	Department of Defense
DODSI	Department of Defense Security Institute
DoE	Department of Energy
DSS	Defense Security Service
EAR	Export Administration Regulation
FBI	Federal Bureau of Investigation
FCL	Facility Security Clearance
FOCI	Foreign Ownership, Control, or Influence
FSC	Federal Supply Code (see CAGE)
FSO	Facility Security Officer
GCA	Government Contracting Activity
ITAR	International Traffic in Arms Regulation
KMP	Key Management Personnel
LAA	Limited Access Authorization
LOC	Letter of Consent (DISCO Form 560)

MFO	Multiple Facility Organization
NISPOM	National Industrial Security Program Operating Manual
PCL	Personnel Security Clearance
PCO	Procuring Contracting Officer
RFI	Representative of a Foreign Interest
UA	User Agency

1. SECURITY EDUCATION

The Facility Security Officer (FSO) shall, on a recurring basis but *not* to exceed one year, bring to the attention of all cleared personnel their continuing responsibility for safeguarding classified information. Each cleared employee shall be made aware of the security procedures that pertain to that employee's particular work assignment and security deficiencies resulting from recurring inspections by the Defense Security Service (DSS) or self-inspections conducted by the FSO. All employees shall be given an initial security briefing that includes briefings on threat awareness, defensive security, and an overview of the security classification system and reporting obligations and requirements. Each cleared employee in possession of classified information shall be informed of his/her responsibility for determining whether a prospective recipient of an item of classified information is an authorized person. The employee releasing the classified information will also be responsible for telling the recipient that unauthorized disclosure of classified information violates Department of Defense (DoD) regulations and contractual obligations and is punishable under the provisions of federal criminal statutes. Information on these subjects is located in the NISPOM, Chapter 3.

2. INDIVIDUAL RESPONSIBILITY

Each cleared employee of Astrotech is required to report to the FSO any of the following:

1. **Espionage** – Information coming to his/her attention concerning existing or threatened espionage, sabotage, or subversive activities at their place of employment where defense work is being performed.
2. **Suspicious Contacts** – Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information. All contacts with known or suspected intelligence officers. Attempted exploitation by intelligence services of another country.
3. **Compromise** – The loss, compromise, or suspected compromise of classified information, within or outside of the Company, regardless of the classification level. In the event the incident occurred outside the Company, the employee would also report the matter to the nearest Federal Bureau of Investigation (FBI).
4. **Adverse Information** – Any information coming to the attention of any employee concerning another employee who is currently cleared or in the process of being cleared for access to classified information, which indicates that such access or determination may *not* be clearly consistent with the national interest. As a general rule, this is information that reflects adversely on the integrity or character of the employee and could suggest that his/her ability to safeguard classified information may/could be impaired. The following are some examples of types of Adverse Information which should be reported to the FSO:
   - Criminal activities
   - Bizarre or notoriously disgraceful conduct
   - Treatment for mental or emotional disorders
   - Excessive use of intoxicants
   - Illegal substance use such as Marijuana, Heroin, Cocaine, or Hashish
   - Excessive indebtedness or recurring financial difficulties

   The above examples are *not* all inclusive. If there is doubt whether something is considered adverse or *not*, report the information to the FSO for a determination.
5. **Foreign Travel/Meetings in ~~Designated~~ Countries** – ~~The intended travel to or through a designated country or attendance at an international scientific, technical, engineering, or other professional meeting regardless of the geographic location, when it can be anticipated that representatives of designated countries will participate or be in attendance. This travel should be reported to the FSO at least 30 days in advance of travel. The FSO is required to provide all travelers with a defensive security briefing and counterintelligence awareness briefing. All travelers must report to the FSO upon their return for a debriefing.~~Whether you are traveling on business or pleasure, foreign travel plans should be reported to your security office at least 2 weeks in advance of your travel. Your security office can provide you with the latest State Department advisories on hazardous conditions, identify any known security concerns regarding the areas where you will be traveling or organizations you will be dealing with, and provide general information on security risks during foreign travel. Following your trip, complete any required post-foreign forms and report any unusual incidents that occurred during your travel.
6. ~~**Name Change/Citizenship** – Any change in legal name. When applicable, any cleared Immigrant Alien who becomes a citizen through naturalization.~~**Change in Personal Status:** Changes in

marital status, cohabitation and change of name must be reported. Special requirements may apply if any intended spouse or partner is a Foreign National.

7. **Representative of a Foreign Interest (RFI)** – Any change in status wherein an employee becomes a Representative of a Foreign Interest (RFI). Such would occur when a citizen of the United States or an Immigrant Alien acts as a representative, official, agent, or employee of a Foreign Government, firm, corporation, or person.
8. **Classified Meetings~~/Communist Visits~~** – The FSO must be notified of all plans to host an unclassified visit by Representatives of ~~designated~~ foreign countries and notified in advance of any classified meetings to take place within the Company.
9. **Public Disclosure** – The fact that information currently classified by the Government has been disseminated by a public medium of communication does *not* automatically mean that it has been declassified. Classification shall be continued until advised to the contrary by the Government. Questions as to the propriety of continued classification should be brought to the immediate attention of the FSO who will forward the question to the appropriate Government CO. Classified information shall *not* be disclosed at any meeting, conference, seminar, symposium, exhibit, or convention except under the conditions described in NISPOM.
10. **Disclosure of U.S. Information to Foreign Interests** – Personnel shall avoid divulging information that has *not* been approved for public disclosure. Disclosure authorization may be in the form of an export license, a letter authorization from U.S. Government licensing authority, or an exemption to the export authorization requirements. Please refer to the International Traffic in Arms Regulation (ITAR) for further information.

3. CLEARANCE PROCEDURES

The FSO shall require each employee who is an applicant for a security clearance and who claims U.S. Citizenship to produce evidence that will verify such citizenship. A record will be made of which document was cited as proof of U.S. Citizenship. Acceptable documents that prove U.S. Citizenship are listed in Section 2 of the NISPOM.

3.1 CONFIDENTIAL / SECRET CLEARANCES

Applications for CONFIDENTIAL/SECRET clearances will be submitted on SF Form 86, "Security Clearance Application," in accordance with Section 2 of the NISPOM. Such clearances may only be granted to U.S. Citizens. The applicant will be afforded privacy in completing Part 2 of this form and the information recorded therein will *not* be made available to the Company or copies retained in the employee's files. When the applicant has applied for or received a previous security clearance, SF Form 562, "Clearance Change Notification," will be submitted with a copy of DISCO Form 560, "Letter of Consent." Applicants for employment will *not* be processed for a security clearance until hired and SF 86's used for processing clearances will *not* be used as a means of screening prospective employees. If there is *no* indication that a prior clearance has been suspended, denied, or revoked, the clearance may be granted.

3.2 FINGERPRINT CARDS

The FD Form 258, "Fingerprint Card," shall be completed prior to completion of the SF Form 86 so that it will be available for the employee to insert in the preaddressed envelope with Part 2. To ensure that the person being fingerprinted is in fact the same as the employee processed for clearance, another Company employee shall witness the taking of fingerprints. The FSO or his/her designated representative shall witness the placing of the fingerprint card in the envelope and the sealing of the envelope to assure substitutions do *not* occur.

3.3 CHANGES IN CLEARANCES

SF Form 562, "Clearance Change Notification," will be utilized to report the termination, transfer, re-employment, downgrading, reinstatement, administrative termination, and change in name on any clearance issued or being processed by DSS. This form will be submitted to DSS. File copies will be retained with the security clearance or clearance application to which they pertain.

4. SECURITY BRIEFINGS

4.1 INITIAL BRIEFING

Employees will read the espionage and sabotage statutes and other applicable federal criminal statutes, in particular Sections 793, 794, 798, and 799, Title 18, U.S. Code. In addition, applicable portions of this Security Manual will also be read. Discussions will be held concerning the individual's responsibility for safeguarding classified information, reporting of incidents and changes to status, the differences in, and the importance of levels of classification. Subsequent to the briefing, each cleared employee will execute Part 10 of Standard Form 312, "Classified Information and Nondisclosure Agreement."

4.2 TERMINATION BRIEFINGS

Employees who are terminating through discharge, resignation, or retirement, or who are entering into a lay-off or leave of absence expected to exceed 120 days, must read and execute the Security Debriefing Acknowledgement portion of the SF312. If the terminating employee has had access to any TOP SECRET (TS), Communications Security (COMSEC), or other information requiring Special Access, an oral debriefing is required in conjunction with the execution of the Security Debriefing Acknowledgement portion of the SF312. The debriefing shall include a statement of:

- purpose of the debriefing,
- serious nature of the subject matter which requires protection in the national interest,
- need for caution and discretion, and
- advice concerning any travel restrictions that are appropriate.

The completed SF 312 will be retained for 50 years.

4.3 REFUSAL TO EXECUTE SF 312

An employee issued an initial PCL must execute a SF 312 prior to being granted access to classified information. The contractor shall forward the executed SF 312 to the CSA for retention. If the employee refuses to execute the SF 312, the contractor shall deny the employee access to classified information and submit a report to the CSA. The SF 312 shall be signed and dated by the employee and witnessed. The employee and witness signature must bear the same date.

5. VISITS

5.1 OUTGOING VISITS

When it becomes necessary for employees of this Company to visit other cleared contractors or Government agencies, and access to classified information or controlled areas is anticipated, the following procedures will apply:

5.1.1 FSO Notification

The FSO must be notified as to the Contractor or Agency to be visited, the time and duration of the visit, the reason for the visit, and the person to be contacted. Ample time must be allowed to permit the visit authorization to be prepared, mailed to the Contractor or Agency, and to be processed by their visitor control section.

5.1.2 Visit Authorization Request

The FSO will prepare a written visit authorization request in accordance with Chapter 6 of the NISPOM. In the event a visit must be arranged on short notice, telephonic authorizations may be obtained provided it is followed by a written request. Unless notified to the contrary by the Contractor or Agency to be visited and sufficient time has elapsed to permit processing of the request, outgoing visit requests may be presumed to be approved.

5.1.3 Visit Authorization Dates

Visit authorizations may be submitted for specific dates or for periods *not* to exceed 12 months. Contract related visits may be arranged for the duration of the contract with the approval of the activity being visited. It is the responsibility of the FSO to cancel all outstanding visit authorizations, in writing, in the event the employee to which they pertain has died, terminated, retired, or *no* longer requires the access originally authorized.

5.2 INCOMING VISITS

In the event that employees of other cleared contractors or of Government agencies make visits to this Company that will require access to classified material or participation in classified discussions, the following procedures will apply:

5.2.1 Visitor Security Clearance Verification

The FSO shall verify each visitor's security clearance status. He/she is responsible for determining that the requesting contractor has been granted an appropriate facility security clearance, based either on an existing contractual relationship involving classified information of the same or higher category, or otherwise by the Clearance Verification Authorization Center at (888) 282-7682. When the requesting contractor's facility security clearance status has been determined, his/her certification as to the proposed visitor's personnel security clearance status may be accepted. If, however, there is any question as to the validity of a visit request or identity of the visitor, appropriate confirmation shall be obtained from the contractor or User Agency activity, which initiated the visit request.

5.2.2 Classified Information Access Conditions

Approved visitors will be afforded access to classified information consistent with the authorized purpose of the visit. Visitors shall be prohibited from making records of classified discussions and taking photographs in areas where classified information might be recorded on the film. Classified material shall *not* be released to a visitor to take outside Company facilities except when authorized by the FSO.

5.2.3 Record Maintenance

The FSO shall maintain a record of all visitors to the Company for the purpose of access to classified information. The record shall indicate:

- visitor's full name;
- name of the contractor or activity he/she represents;
- date and time of their arrival and departure; and
- citizenship.

5.3 Foreign Visitors -The Customer Program Manager will forward to the Astrotech FSO a completed Access and Badging Request form (**SHI-ASO-F0025**) a minimum of one week in advance of any Foreign Nationals visiting the Astrotech Florida Facility. The Astrotech FSO will check the list of Foreign Nationals against the U.S. Denied Persons list to make sure that the Foreign Nationals have been permitted legal entry into the United States. This list of approved visitors is maintained by the Astrotech FSO and updated with the Astrotech entry control point on a daily basis.

5.3.1 Foreign National Visitor Badging: Upon arrival at the Astrotech Florida Facility, the Foreign National visitor will sign in at the entry control point, show proof of citizenship and be given an Astrotech Visitor's Access Badge. For Foreign Nationals, this badge is goldenrod in color and clearly indicates that the visitor is a Foreign National.

5.3.2 Foreign National Visitor Access – Unescorted: Foreign Nationals will have unescorted access to the non-secure areas of the Astrotech Florida Facility, including the Astrotech administrative areas, bathrooms, break rooms, outside areas, etc. The offices of the Astrotech technical staff are secured when unoccupied. All program work areas (office areas, control rooms and clean work areas) are secured for restricted personnel access through the use of cipher locks. Each program manager controls access to his/her specific program areas through control of the cipher combinations. The combinations to the locks are selected by the program manager.

5.3.3 Foreign National Visitor Access – Escorted: Foreign nationals are provided access to program work areas for the specific program they are supporting by the program manager, based on employee work requirements and need-to-know. Visitor escorts, if required within the program work area, are the requirement of the program.

5.3.4 Foreign National Visitor Briefing: Astrotech personnel are briefed on mission-specific security and export control procedures prior to the start of each mission involving foreign national customers.

6. FACILITY SECURITY OFFICER (FSO) RESPONSIBILITIES

The FSO of this Company is responsible for performing the following functions:

1. Supervise and direct security measures necessary for implementing the NISPOM and related Federal requirements for classified information. The FSO, or those otherwise performing security duties, shall complete security training as specified in Chapter 3 of the NISPOM and as deemed appropriate by the CSA.
2. Maintain all facility clearance records, to include "Letter of Notification of Facility Security Clearance;" DD Form 441 or 441-1, "Department of Defense Security Agreement;" and DD Form 441s, "Certificate Pertaining to Foreign Interests," if applicable.
3. Maintain all personnel security clearance records, to include DISCO Form 560, "Letter of Consent;" and SF Form 86, "Application and Authorization for Access to Classified Information." Furthermore, the FSO shall be responsible for verifying security clearance of all Company personnel.
4. Maintain the National Industrial Security Program Operating Manual for Safeguarding Classified Information (NISPOM), DoD 5220.22-S-2 and preparing, maintaining and distributing this Security Manual to implement, within the Company, the applicable requirements of the NISPOM. Also to revise the Security Manual, as necessary, and to implement the revisions applicable to the Company's operation within four months of a receipt of a revision of the NISPOM.
5. Prepare, after receiving notice of a forthcoming security inspection by the Government, a listing of all classified contracts on which the Company is currently performing.
6. Indoctrinate all cleared employees as to their individual responsibilities for safeguarding classified information; and at time of clearance and/or termination, obtain execution of Standard Form 312, "Classified Information Nondisclosure Agreement."
7. Process requests for SECRET clearances on SF Form 86, "Security Clearance Application," or SF Form 562, "Clearance Change Notification."
8. Conduct a self-inspection program for the purpose of evaluating all security procedures applicable to this Company. The security system shall be subject to continuous review, and a formal self-inspection shall be conducted approximately midway between scheduled government inspections. The self-inspection will include all elements of this Company's security program, and corrective action will be accomplished as expeditiously as possible on any deficiency identified as a result of the inspection. A record of the date upon which the self-inspection was accomplished shall be maintained, and this record must be available for review during the next regularly scheduled inspection by the CSA.
9. Receive, prepare, and submit, immediately in writing, to the CSA or DSS, as appropriate, all the reports required by Section 1 of the NISPOM. Principal reports required are:
    a. Actual or suspected espionage, sabotage, or subversive activity at any Company location or involving any Company personnel. The primary recipient of this report is the nearest field office of the Federal Bureau of Investigation (FBI) and an information copy is to be sent to the CSA.

b. Actual or suspected loss or compromise of classified information and/or material, regardless of the level of classification.

c. Any violation of the NISPOM involving Restricted Data, Formerly Restricted Data, or other special access information.

d. Any change conditions within the Company related to ownership, operating name or address, foreign interests, or termination of business.

e. Additions, deletions, or any changes in the Key Management Personnel (KMP) within the Company, and complete details regarding replacement.

f. Termination, death, change of name, lay-off, or leave of absence in excess of 120 days, of any employee cleared or pending clearance by DSS.

g. Refusal of any cleared employee to execute either part of the SF 312, when requested to do so.

h. Any adverse information of substance concerning the loyalty or suitability of cleared employees or those undergoing clearance processing.

i. Acquisition by any cleared personnel, or those undergoing clearance processing, or relationships in or with designated countries.

j. Naturalization of a cleared Immigrant Alien. This report is submitted on DISCO Form 562.

k. Circumstances under which cleared personnel, or those in process for a clearance, become representative of a foreign interest, or whose status such as a representative changes adversely.

l. A report upon notification by an employee that he/she no longer wishes to be processed for a clearance, or to continue an existing personnel security clearance.

m. A report of any cleared Immigrant Alien who has been assigned or taken residence outside the U.S. for a period in excess of 90 consecutive calendar days in any 12-month period. Visits in excess of 90 consecutive days invalidate any existing security clearance.

n. The intent to host an unclassified visit by representatives or nationals of a designated country as soon as the visit arrangements are known.

o. The briefing of cleared personnel who will have contact with representatives or nationals of a designated country at a visit hosted by this Company.

10. Ensure that classified information is furnished or released only to authorized persons. Public disclosure of information pertaining to classified contracts or projects shall be in accordance with the security requirements received from the CO. Brochures, promotional sales literature, or similar type material containing classified information shall *not* be published or distributed without prior review and written authorization by the CO. Classified information shall *not* be disclosed in any manner at a meeting, conference, seminar, symposium, exhibit, or convention except under the following conditions:

    a. At a meeting conducted pursuant to and as a necessary element of a specific contract held only in the prime or subcontractor's facility and attended only by authorized persons who have a need-to-know in connection with the contract; and over which meeting controls have been established to ensure that the meeting site is physically secure, that the classified notes, minutes, and

summaries resulting from the meeting are properly safeguarded, and that the attendees are given sufficient classification guidance during the oral presentations.

b. At a meeting conducted by a DoD activity, provided, that, when the information to be disclosed is under the jurisdiction of another Government agency or when the meeting is to be attended by representatives outside the DoD, the contractor requests the conducting activity to obtain written approval from the CO concerned prior to the disclosure. A copy of such request shall be furnished to the CO concerned. The contractor is *not* required to obtain approval if only DoD information is to be disclosed and only contractor, subcontractors, their employees, and DoD personnel are to attend the meeting.

c. At a meeting conducted by a contractor, association, institute, or society whose membership is composed primarily of contractors cleared by the DoD, contractor employees, or DoD personnel, and sponsored for security purposes by the DoD, provided written approval of the CO concerned is furnished to the sponsoring activity prior to the disclosure.

d. At a meeting conducted or sponsored by Government agencies other than the DoD, provided the contractor requests and obtains written approval from the CO prior to the disclosure. Security sponsorship of a meeting at a User Agency other that the DoD will be in accordance with the provisions of that agency. However, as a minimum, the requirements of the NISPOM shall apply for the safeguarding of classified information.

7. CLASSIFIED INFORMATION STORAGE

When *not* in use and safeguarded as prescribed in Chapter 5 of the NISPOM, classified material received by or in the possession of the Company at this facility shall be stored as follows:

7.1 SECRET / CONFIDENTIAL MATERIAL

SECRET and CONFIDENTIAL material shall be stored in the GSA approved Mosler security container, bearing a GSA Test Certification Label, located in the FSO's Office.

- Only a minimum number of authorized persons shall possess the combination to the cabinet or have access to the information stored therein.
- A record shall be maintained of the names and addresses of all persons having knowledge of the combination.
- The cabinet shall be kept locked when *not* under the direct supervision of an authorized person entrusted with the combination or the contents.
- The combination to the cabinet shall be classified to the highest level of material contained therein.
- Authorized persons will be required to memorize the combination and *no* written record of it shall be established.

7.2 COMBINATION

The combination to the container shall be changed at least once every year and at the earliest practical time following:

- reassignment, transfer, or termination of any person having knowledge of the combination or when the PCL granted to any such person is downgraded to a level lower than SECRET, or is suspended or revoked by proper authority;
- compromise or suspected compromise of the cabinet or its combination, or the discovery of the cabinet being left unlocked and unattended; or
- initial receipt of the cabinet.

Only the FSO or his/her designated representative shall change the combination to the cabinet. Removal of classified material by Company employees for use or storage at a private residence is *not* authorized.

7.3 OVERNIGHT STORAGE OF HAND-CARRIED CLASSIFIED MATERIAL

When employees of the Company are required to hand-carry classified material on trips that involve an overnight stopover, arrangements must be made by the FSO in advance of departure for overnight storage of the hand-carried classified material in a U.S. Government installation or a cleared contractor's facility.

8. CONTROL OF AREAS

Classified material will normally be protected in the manner described in Section 7 of this manual. If, however, because of the nature, size, or characteristics of the classified material, safeguarding will be by controlling the area in which it is located. The entry into a controlled area will *not* necessarily constitute access to classified information if the security measures that are in force prevent the gaining of knowledge of the classified information. Therefore, the entry into a controlled area under conditions that prevent the gaining of knowledge of classified information will *not* necessitate a personal security clearance.

1. A controlled area shall *not* be established for the purpose of storing classified documents.
2. The CSO and Astrotech shall agree on the need to establish, and the extent of the controlled area at such times when the need for controlled areas becomes apparent during the performance of a contract.
3. The CSO shall be advised in accordance with Section 8, Chapter 5 of the NISPOM of the establishment of any new controlled areas or any change in the location or extent of existing controlled areas. Controlled areas that have been temporarily deactivated and then subsequently reactivated within 180 days need *not* be reported.
4. A controlled area shall be disestablished when the original or existing need for the creation of the area *no* longer exists, and there is *no* anticipated need for the area within 180 days.
5. A physical barrier capable of preventing unauthorized entry shall separate closed areas from adjacent areas, and when visual access is a factor, observation by unauthorized persons. The barriers shall protect against surreptitious or forced entry, and shall be constructed to offer visual evidence of forced or attempted forced entry.
6. Access to an unlocked entrance to a controlled area during working hours for material classified *no* higher than SECRET shall be controlled by a properly cleared Astrotech-authorized guard stationed to supervise the entrance or by properly cleared and briefed contractor personnel.
7. Access to a locked entrance to a controlled area during working hours for material classified *no* higher than SECRET shall be controlled by the FSO or his/her designee or by properly cleared and briefed contractor personnel stationed to supervise the entrance. The FSO/contractor shall be required to unlock the entrance, remain at the entrance while it remains open, supervise the passage of material or authorized personnel through the entrance, and to lock it immediately thereafter.
8. Access to a controlled area during non-working hours for material classified *no* higher than SECRET shall be controlled by locked entrances and exits secured with a dial-type changeable combination padlock as described in Chapter 5 of the NISPOM. Doors secured from the inside with panic bars, or electric drive controls and their manual drive backups (i.e., rollup doors) will *not* require additional locking devices.
9. If SECRET information is stored in the area during non-working hours, the last cleared individual in the area will thoroughly check the area and sign a log posted on the inside of the door indicating that no one remains within. An Astrotech-authorized guard shall patrol the area and provide a written record of coverage of key points outside the area. Such patrols shall take place once every three hours and shall include visual inspections of all exterior doors. The guard shall certify by signature

on a log posted on each door that the door was checked and found to be locked during the course of the patrol.

10. All areas designated as closed areas shall be designated as such with appropriate signs.
11. Persons assigned to the area shall challenge the presence of any unknown person and establish that individual's need-to-know.
12. Construction of closed areas shall be in accordance with the provisions of Chapter 5, Section 8 of the NISPOM and/or written guidance of the CSA.

9. CLASSIFIED MATERIAL TRANSMISSION

9.1 MAILING OF CLASSIFIED MATERIAL (OUTGOING)

Classified material that is intended to be dispatched to another cleared site will be shipped as follows:

1. SECRET material must be sent via U.S. Registered Mail or other approved methods as described in Chapter 5 section 4 of the NISPOM. CONFIDENTIAL material may be sent by U.S. Express Mail or U.S. Certified Mail.
2. The inner and outer cover shall be enclosed in opaque paper and shall be sealed with tamper resistant tape.
3. The inner wrapper shall be plainly marked with the assigned classification and addresses of both the sender and addressee.
4. The outer cover shall be sealed and addressed with *no* identification of the classification of its contents.
5. A receipt shall be attached to or enclosed in the inner cover (CONFIDENTIAL information shall require a receipt only if the sender deems it necessary).
   - The receipt shall identify the classified contents and the name and address of both sending and receiving facilities.
   - Receipts shall *not* contain classified information. A short title or abbreviation shall be substituted for a classified title.
   - A duplicate copy of the receipt shall be retained in a suspense file until the signed copy is returned.
   - A suspense date (normally *not* to exceed thirty days) shall be established and follow-up action shall be initiated if the signed receipt is *not* returned within that period.
   - If, after the follow-up action, a signed receipt is still *not* returned or the addressee indicates non-receipt of the classified material, an inquiry shall be conducted in accordance with the NISPOM.
6. This package shall then be presented to the U.S. Postal Service for mailing by Registered Mail, Return Receipt Requested, or another approved carrier.
7. The COMSEC Custodian shall retain copies of signed receipts for classified material for a minimum of two years.

9.2 COURIER PROCEDURES

The normal method for transmitting classified material to another cleared facility is by an approved method as stated in Chapter 5 section 4 of the NISPOM; but occasionally, due to urgency, classified material may have to be hand-carried to another site. The FSO must approve all courier authorizations. He/she must perform the following:

1. Verify the facility clearance and storage capability of the receiving site.
2. Forward the courier's clearance to the receiving site.
3. Package the material as if it were being mailed.

4. Prepare a courier letter in accordance with NISPOM, Chapter 5 describing both the courier and the package.
5. Prepare a hand receipt for the courier that describes the classified material by its unclassified title and document control number. A receipt is *not* required for CONFIDENTIAL material.
6. Hand-carrying classified hardware, and other bulky packages, aboard commercial passenger aircraft must be approved by the CSO on a case-by-case basis. Call the CSO for instructions.
7. Once these actions are completed, the courier will sign for the package on a hand receipt. The package must remain in the possession of the courier or be stored in an approved security container at a cleared facility at all times.

9.3 CLASSIFIED MATERIAL CONTROL (INCOMING)

In order to ensure the proper control and safeguarding of classified material, the Company will follow these procedures:

1. The FSO will be custodian of all classified material held by the Company.
2. The FSO will maintain records of all SECRET material handled by the Company. These records will include:
   a. receipt or origin;
   b. activity from which received or originated;
   c. classification of the material;
   d. brief, unclassified description of the material; and
   e. disposition of the material and the date thereof.

   These records shall be maintained for two years from the date that the last item recorded there on was disposed of. Receipt and dispatch records will be maintained for CONFIDENTIAL material and must include a, b, c, d, and e above.
3. Classified material will be secured in the Company's security container unless it is in actual use by authorized personnel. When in use, classified material will be protected as follows:
   a. It will be kept under the constant surveillance of an authorized person who is in a physical position to exercise direct security controls over the material.
   b. It will be covered, turned face down, placed in the Company's storage cabinet, or otherwise protected when unauthorized persons are present.
   c. It will be returned to the security container as soon as practical after use.

9.4 CLASSIFIED MATERIAL CONTROL (OUTGOING)

The Company will *not* release classified material without the approval of the CO except in the following instances:

1. When release is required by the specific terms of the contract.
2. When it is necessary in the performance of the contract.

3. In connection with pre-contract negotiations with prospective subcontractors, vendors, or suppliers.
4. In prime contractor-subcontractor, Multiple Facility Organization (MFO), and parent-subsidiary relationships as authorized by the NISPOM.
5. During visits among prime contractors that are participating under U.S. Government direction in contracts pertaining to research, development, or production of a weapon system.

9.5 AUTOMATIC DATA PROCESSING (ADP) USE

The Company will *not* use Automatic Data Processing (ADP) in the processing of classified information until the ADP system has been approved by the CSO.

10. CLASSIFIED MATERIAL REPRODUCTION

Classified information will only be reproduced on copy equipment that has been approved for classified reproduction. Procedures for classified reproduction will be posted by approved equipment.

11. MATERIAL CLASSIFICATION

11.1 COMPANY-GENERATED MATERIAL CLASSIFICATION

It may be necessary, in the performance of a contract, for the Company to classify material that has been generated by the Company. The following procedures will apply to this process:

1. The CO or his/her representative will supply the security classification applied to material involved with User Agency contracts and programs using the "Contract Security Classification Specification," DD Form 254. Classification of material produced by the Company in the performance of such a contract or program will be in accordance with the Company's knowledge that the material produced is in substance the same as, or would reveal, other information know to be currently classified.
2. Whenever the Company originates information *not* in the performance of a User Agency contract or program, it is to be classified if the Company already knows it is classified.
3. If the Company originates information that it thinks may or should be safeguarded, it will protect the information as though classified at the appropriate level until an advisory classification opinion is obtained from a User Agency that has an interest in the subject matter.
4. Within the Company, the responsibility for classifying and marking material lies with the manager or supervisor whose signature or other form of approval is required in order that the material be transmitted.

11.2 CLASSIFIED MATERIAL ORIGINATION PROCEDURES

When the Company is involved in the generation of classified documents or material, the following procedures will be followed:

1. The creation of a finished document involves a phase in which working papers such as notes, drafts, and drawings are prepared. These working papers need *not* have the full range of classification markings of a finished document. They are only required to have the overall classification markings on the first and last page and the individual page markings on the interior pages.
2. Papers must be fully marked if they are entered into the accountability records, made a part of a permanent record, or transmitted outside the facility.
3. When the Company prepares classified documents, these must be entered into the accountability records when the first of any of the following events occurs:
    a. Document is retained as a completed document in excess of 30 days from the date of completion.
    b. Document is reproduced for internal purposes.
    c. Document is retained as a partially completed document on discontinuance of the work.
    d. Document, regardless of its stage of development, is transmitted outside of the facility.

11.3 ACCOUNTABILITY

When a classified document or other material is joined to, incorporated in, or otherwise made a part of another classified document or item of material, accountability for the incorporated document or item

shall be terminated, and accountability for the document or item in which it was incorporated shall be established.

11.4 TYPING

When typing classified documents, uncleared personnel will be kept out of the area.

11.5 RIBBONS/CARBONS

Ribbons and carbons used in the preparation of a classified document will be stored in the security container at the end of each classified typing session. Ribbons shall be marked with their overall classification.

11.6 DOCUMENT PREPARATION BY-PRODUCT DESTRUCTION

Carbons, rejects, and other by-products of the document preparation process need *not* be marked with the usual classification markings but shall be destroyed at the earliest practical moment.

11.7 WORD PROCESSORS/MEMORY TYPEWRITER PRIOR APPROVAL

The Company will *not* use word processors and memory typewriters for preparing classified information unless the system has been approved by the CSO.

12. MARKINGS

Classified material will be marked in accordance with the NISPOM. The Security Officer will ensure that all classified material is properly marked and will brief those individuals who will generate information on the proper marking requirements.

13. CLASSIFIED MATERIAL DESTRUCTION OR DISPOSITION

13.1 DISPOSITION / DESTRUCTION

It is the policy of the Government and shall be the policy of the Company to minimize the quantity of classified information on hand. Once classified material has served its purpose it should, at the earliest practical moment, be returned to its originator or destroyed in the following way:

1. Classified documents will be destroyed by burning or returned to the sending contractor/agency.
2. Two appropriately cleared employees of the Company must witness the burning of SECRET material.
3. The burning of CONFIDENTIAL material requires only one witness.
4. When SECRET material is burned, a destruction certificate will be prepared and signed by both employees. This certificate will contain the date of destruction and a description of the material destroyed.

13.2 ACCOUNTABILITY RECORDS

The FSO will maintain accountability records reflecting the destruction of the material.

14. EMERGENCY PROCEDURES

This section specifies procedures to be followed for the protection of classified material in the event of a natural disaster or civil disturbance.

1. Individual employees shall ensure that all classified material is locked in security containers.
2. Notify FSO immediately.
3. If evacuation of the area or building is required, upon return an inventory shall be performed of all classified material in any damaged area. The Security Officer must submit reports of any espionage, sabotage, or subversive activities; and any loss, compromise, or suspected compromise of classified information to the cognizant security office.
4. The FSO shall request any required assistance from appropriate civil authorities, including local and State law enforcement agencies.
5. In the event of any emergency situation, which threatens the security of classified information, we must notify the following offices immediately.
   - Identify yourself and your facility using Commercial and Government Entity (CAGE) code.
   - Indicate that the facility is a cleared facility under the Defense Industrial Security Program and that you have an emergency situation and need guidance as to what action should be taken.

